BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
Examination of Current Policy Concerning the Treatment of Confidential Information Submitted to the Commission	)	GC Docket No. 96-55

BRIEF OF SBC COMMUNICATIONS INC.

JAMES D. ELLIS
ROBERT M. LYNCH
DAVID F. BROWN

175 E. Houston, Room 1254
San Antonio, Texas 78205
(210) 351-3478

ATTORNEYS FOR SBC
COMMUNICATIONS INC.

DURWARD D. DUPRE
MARY W. MARKS
J. PAUL WALTERS, JR.
One Bell Center, Room 3520
St. Louis, Missouri 63101
(314) 235-2507

June 14, 1996

GC Docket No. 96-55

BRIEF OF SBC COMMUNICATIONS INC.

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington. D.C 20554

In the Matter of	)	
	)	
Examination of Current Policy	)	GC Docket No. 96-55
Concerning the Treatment of	)	
Confidential Information	)	
Submitted to the Commission	)	

BRIEF OF SBC COMMUNICATIONS INC.

SUMMARY

With passage of the Telecommunications Act of 1996 (Act), SBC Communications Inc. ("SBC")[1] faces increased competition for all of its services. Confidential and proprietary business information that SBC could once submit to the Commission under limited protection must now be rigorously protected.

The Commission has instituted this Notice of Inquiry and Notice of Proposed Rulemaking (NPRM) to determine "how to avoid unnecessary competitive harm that could be caused by the disclosures of such information and still fulfill our regulatory duties in a manner that is efficient and fair to the parties and members of the public who have an interest in our proceedings."[2]

---

[1] SBC Communications Inc. files on behalf of its subsidiaries, Southwestern Bell Communications Services, Inc. ("SBCS"), Southwestern Bell Telephone Company ("SWBT") and Southwestern Bell Mobile Systems ("SBMS").

[2] Notice of Inquiry and Notice of Proposed Rulemaking, GC Docket No. 96-55, ¶1, released March 25, 1996.

The key issue to be decided is the extent of the Commission's "regulatory duties" under the Act. As evidenced in the Telecommunications Act of 1996, Congress intends for competition to replace regulation. The Commission's regulatory duties, therefore, primarily consist of allowing the market to function. The Commission should focus on streamlining the regulatory process as directed by Congress. Moreover, because of the evolution from regulation to competition in the telecommunications industry, the Commission should abstain from compelling industry participants to routinely file confidential information that they would not make generally available to the public on a voluntary basis. The presumption should now be that a carrier's confidential information will remain confidential.

I. TARIFFING PROCEDURES

The treatment of competitively sensitive information was an important issue for SWBT even before the passage of the Telecommunications Act of 1996. The Expanded Interconnection Orders, which required all Tier 1 local exchange carriers ("LECs") to offer physical collocation and ultimately virtual collocation, greatly increased competition for interstate access services. SWBT's Expanded Interconnection filings requested confidential treatment of SWBT's cost support to protect confidentially negotiated equipment vendor prices as well as costs and overhead factors for its DS1 and DS3 services. In a November 1, 1994, ruling, the Common Carrier Bureau found sufficient reasons to qualify SWBT's cost support under Exemption 4 of the Freedom of Information Act (FOIA). However, SWBT sought review of the ruling because it allowed broad disclosure of the data to an almost limitless number of people under the terms of a protective order,

similar to Attachment A to this NPRM, without any penalties for accidental or purposeful disclosure. SWBT's Application for Review of the Bureau's November 1, 1994, ruling is still pending.

Since the Bureau's ruling, SWBT has tariffed a number of competitive services and has been granted confidential treatment of the cost support. In each instance, SWBT demonstrated that competitors offer the same or similar service, and in each case the Bureau found good cause to waive Sections 0.453(j) and 0.455(b)(11) of the Commission's rules. SWBT met the competitive threshold as determined by the Bureau for DS1 service, DS3 service, ISDN, SONET, fiber optic rings, Operator Services, as well as virtual collocation restructure.

The Commission correctly points out the problems that will occur when incumbent LECs ("ILECs") begin to tariff services requesting a 7 or 15 day effective date. The new streamlining now required by the Act cannot be molded into the Commission's old rules. Requiring advance approval for confidential treatment of cost data, for instance, will only serve to increase the delays that already exist in the tariffing process. ILECs' competitors would then have two opportunities to delay the introduction of a new service, (i.e., advance approval for confidential treatment and petitions to reject the tariff), thus thwarting the intent of Congress. When Congress streamlined Section 203 of the Act, it envisioned that ILECs would be able to make their services available to the public in a more reasonable timeframe. Congress never contemplated that the Commission would create more rules that would essentially delay the offering of the service even longer.

The NPRM asks whether the Commission should "continue to make exceptions to the Commission's rule requiring such data to be made publicly available."[3] The answer to this question requires a closer examination of what the Act, the FOIA and the Commission's Rules actually require.[4]

The Communications Act does not require cost support data to be submitted with tariffs, nor does it require that data, if submitted, be made public. The only requirement in the Commission's Rules that cost support data be made public is found in Section 0.455(b)(11), which requires the Commission to make available for inspection "Tariff schedules for all charges for interstate and foreign wire or radio communications filed pursuant to section 203 of the Communications Act, all documents filed in connection therewith, and all communications related thereto."

The FOIA authorizes the Commission to allow cost support data to remain confidential if the party seeking confidential treatment, in its judgment, satisfies 5 U.S.C. §552(b)(4), part of the FOIA, which protects "trade secrets or commercial and financial information obtained from a person and privileged or confidential." Under the Commission's policies, however, the burden of proof is effectively placed upon the party seeking confidential treatment, who must show,

---

[3] NPRM at ¶44.

[4] The NPRM claims that the Commission has the authority to disclose materials that would otherwise be protected from disclosure by the Trade Secrets Act. The NPRM reads Chrysler Corporation v. Brown, 441 U.S. 281 (1979) to authorize this practice. Such a reading may be overbroad as neither Chrysler Corp. nor CNA FIN. Corp. v. Donovan, 830 F.2d 1132 (D.C. Cir. 1987) cert. denied, 485 U.S. 977 (1988) appear to authorize any broad power in this regard on behalf of the Commission. If taken to an extreme, such a reading could allow the Commission to effectively shield itself from application of the Trade Secrets Act, a result obviously not intended by FOIA.

by a preponderance of the evidence, that disclosure of cost support data will harm substantially that party's competitive position.

These rules were developed before the advent of competition in local exchange and exchange access services. When ILECs were the sole providers of local exchange and exchange access services in their authorized territories, making cost support data available for public inspection may have been a reasonable approach. However, that time has long since passed.

"Public interest" in the context of ILEC interstate services is not necessarily synonymous with interexchange carrier (IXC) interests. IXCs can use the regulatory process to prevent the availability of a better grade of service to a competitor. IXCs or other LEC competitors can also use the process to delay ILEC provision of a new service to an end user to "buy time" to offer a competitive alternative.

The Commission should not ignore the unique characteristics of the access marketplace in resolving this issue. ILECs provide access service in competition with competitive access providers (CAPs) and IXCs and, with the passage of the Telecommunications Act of 1996, many other entrants. The Commission must distinguish between public interest and special interest. Competitors, however, are pursuing ILEC cost data in furtherance of their special interests, not the general public interest. The Commission must not ignore the fact that opposition to confidential treatment of cost data has come solely from entities in competition with ILECs.

As has been demonstrated, competition already exists for many ILEC services, and actual and potential competitors would like nothing better than to review the cost data used to price the service. If an ILEC's costs become public information, all competing firms will have valuable information on which to base pricing and market entry decisions. ILEC competitors are thereby

equipped to capture ILEC customers without risk of competitive response from the ILEC because they will know the ILEC's price floor in advance. ILEC cost data should not be made available to ILEC competitors, any more than competitors' cost data should be made available to ILECs. This principle applies not only to ILECs, such as SWBT, but to all telecommunications competitors.

Success in the marketplace should be driven by technological innovation, service quality, pricing decisions and responsiveness to consumer needs -- not by regulatory strategies designed to obtain a competitive advantage based upon unfairly acquired information. In the current competitive environment, it is often impossible to determine the true motives of those who argue for public disclosure of SWBT's cost data. An access customer may also be a local exchange competitor. There is no way to determine which hat the opposition is wearing at any given time. Is it a customer or competitor? The more competitive the market becomes, the more sensitive the costing, pricing and marketing data will become.

Although the Competitive Pricing Division has recently granted several requests that cost data remain confidential, in each case the decision constituted a waiver of Section 0.453(j) and Section 0.455(b)(11) of the rules. This procedure is unnecessarily and harmfully cumbersome for ILECs, their customers and vendors, as well as for the Commission. It imposes direct and indirect costs on customers by delaying the availability of new services and reductions in rates. The Commission's Rules should be revised to reflect marketplace realities.

ILECs should no longer be required to support tariff filings with cost data. Competition will ensure that prices are reasonable. If they are not, customers can seek remedial action after a tariff becomes effective or simply seek another provider. Aggrieved parties can still avail themselves of the Commission's complaint process to seek a determination of the lawfulness

of any tariff filing. In addition, the Commission is not precluded from investigating and finding unlawful any tariff after it is filed. Elimination of the cost support requirement would do more than any other act to maintain the confidentiality of cost information. Most importantly, it would completely eliminate the need for protective orders -- their attendant controversies and burdensome processes.

If the Commission does not revise its Rules to eliminate the submission of cost support, then the Commission should end the presumption that cost data should be made public unless the filing party can show, by a preponderance of the evidence, that it will suffer significant competitive harm.

Commission Rules should be amended to state specifically that a carrier's cost data will be presumed to be confidential. Carriers should not be required to request confidential treatment with each tariff filing, and the Commission should not waste valuable resources addressing each request. For example, if an ILEC makes a tariff filing, the cost data should be redacted from the public version and disclosed only to the Commission staff. Parties requesting public dissemination of cost information should be required to state compelling arguments for release of the information. Requesting parties should state what deficiency they believe public disclosure will uncover, along with a conclusion as to the harm they will incur if disclosure is not granted.[5] Unless the Commission specifically requests a response from the ILEC, the tariff should automatically take effect and the cost data should remain confidential.

---

[5] The NPRM, at paragraph 24, discusses the standard which the Commission should apply. "Specific and concrete public benefits [must] be reasonably anticipated before properly exempt information will be released on a discretionary basis."

Such a procedure would be in concert with Congressional intent and would allow ILECs to respond effectively to their customers, just as their competitors are allowed to do. It would also improve the speed and quality of Commission service to the public.

II. PROTECTIVE ORDERS

As a general principle, the public should not have access to confidential information as a result of a governmental agency compelling production if that information would not otherwise be available. However, if the Commission requires disclosure of confidential information and a dispute arises, then the Commission has sometimes issued "protective orders," which require that certain information be made available to a requesting party, but limit the party's use of that information. Protective orders are effective only if they afford the level of protection required by specific categories of confidential information. If they do not afford the necessary protection, such orders confer an undue and unreasonable competitive advantage upon the requesting party.

The NPRM includes a draft protective order, which, unfortunately, fails to provide a reasonable level of protection. Specifically, the draft order does not recognize that different types of data should be afforded different levels of confidentiality; instead, the draft order treats all data the same.

A good example of a document which does properly recognize different levels of confidentiality is the model protective order used by the Texas Public Utility Commission (PUC), a copy of which is attached as Exhibit A. This document recognizes both "Confidential Information"

and "Highly Sensitive Confidential Information."[6] Confidential Information is made available, through two copies, only to opposing counsel and witnesses working under the supervision of opposing counsel. Highly Sensitive Confidential Information, on the other hand, is made available only at the offices of the producing party. Opposing counsel may take only limited notes and may make no copies. If the Highly Sensitive Confidential Information involves "competitive information that could be utilized by competitors so as to place the producing party at a significant disadvantage," then production to a competitor is limited to opposing counsel and outside consultants. Both counsel and consultants are expressly prohibited "from disclosing the content of the Highly Sensitive Confidential Information to the competitor or non-regulatory employees of the competitor."

State utility commissions realized long ago that competitors employ discovery, in regulatory proceedings, for business advantage. The standard protective order of the Texas PUC, and similar procedures in SWBT's other states, recognizes this fact and provides appropriate protection.

The Commission's draft protective order, on the other hand, is written as though no competitor would ever seek confidential information for business advantage. The draft order, for instance, allows competitors to copy all data. Indeed, the draft order does not even limit the number of copies which can be made. The draft order also insufficiently restricts the number of people who may examine data. And, for reasons unexplained, the draft order would require a producing party

---

[6] The Texas protective order also recognizes a third category of data needing protection: "Highly Sensitive Confidential Information--Restricted." Production of data included within this category is restricted solely to the PUC.

to maintain confidential information in at least two locations. State commissions typically require that confidential information be maintained only at a single site.

Even the greater protection afforded by state protective orders has not deterred some competitors from using produced data for business advantage. In a very recent proceeding before the Missouri Public Service Commission, SWBT's confidential and proprietary information was distributed and used in violation of a specific protective order, which allowed the data to be distributed only to the counsel and experts of Sprint, the requesting party. Internal Sprint personnel were prohibited from access to the data. The subsequent pre-filed testimony of an internal company witness, however, contained specific references to the protected data. The witness later admitted that he had received copies of all the protected information.

Another serious breach of a protective order occurred in Texas PUC Docket No. 9960, in which an employee of a consultant to CENTEX Telemanagement, Inc. carried data marked "Highly Sensitive Confidential Information" from Texas to California, then made a copy. The information was immensely valuable to SWBT, its competitors, and telecommunications consultants. Although the Texas PUC granted SWBT's motion for sanctions and prohibited the consultant from testifying, the damage was already done.

In another recent example, an IXC employee, during a conference call with SWBT to discuss access rates, claimed that he could determine whether certain SWBT services were cost-based by referring to data produced by SWBT in a Texas docket. This employee had filed testimony in the Texas proceeding and had signed a protective agreement not to use the information outside that particular docket.

These representative examples demonstrate that protective orders, no matter how restrictive, can and will be violated, whether intentionally or by accident. Moreover, as competition increases, the frequency of violations will also increase. If the Commission's Rules are revised as proposed herein, however, there will be no need for protective orders.

III. AUDITS

The NPRM implies that during audits the Commission expects carriers to submit specific requests for confidentiality, as illustrated by the following:.

> In the past, we have normally allowed submitters to request confidentiality for such [audit] data and have dealt with such requests on a case-by-case basis, consistent with the applicable standards in FOIA.[7]

Typically, however, the Commission has not required carriers, during audits, to submit specific and formal confidentiality requests, primarily because such requests would make audits incredibly cumbersome and inefficient. Generally, the Commission has presumed that audit-derived information is not "routinely available for public inspection."[8] This presumption has been based on Section 220(f) of the Communications Act and on the "impairment prong" of the National Parks test,[9] which allow the FCC to withhold information under FOIA exemption 4 if disclosure is "likely . . . to impair the Government's ability to obtain necessary information in the future."[10]

---

[7] NPRM at ¶52.

[8] Scott J. Rafferty, 5 FCC Rcd 4138 (1990).

[9] National Parks and Conservation Ass'n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

[10] The "third prong" of the exemption 4 test, discussed in paragraph seven of the NPRM, would also support a presumption that audit-derived information is exempt from disclosure. The (continued...)

During an audit, the Commission may send the carrier dozens of separate written data requests. Requiring the carrier to submit Section 0.459 confidentiality requests in advance is unnecessary in view of the Commission's general position regarding audit-derived information. In addition, requiring the carrier to submit a separate confidentiality request, after the fact, to cover each item sought would be totally unworkable, particularly when Commission auditors orally request information during on-site visits. For these reasons, the Commission should specifically state in this docket that audit-derived information will not routinely be made available for public inspection.

Similarly, protective orders are not needed in audits. Historically, the Commission, when departing from its long-standing practice of protecting the confidentiality of audit-derived information, has limited disclosure to a summary or report, and then only to inform the public. If the Commission maintains this practice, as it should, protective orders would be unnecessary. Of course, before an audit report or summary is published at the conclusion of an audit, the Commission should allow the audited carrier an opportunity to object (pursuant to appropriate FOIA procedures) to disclosure of any confidential information.[11]

The Telecommunications Act of 1996, at Section 220(c), authorizes the Commission to employ independent third-parties to conduct carrier audits. Section 220(c) also requires all independent auditors to protect carriers' proprietary information. The Commission should specifically inform all independent auditors, in writing, of this duty. The Commission should also

---

[10](...continued)
third prong would allow the Commission to withhold audit-derived information to protect the Commission's interest in an efficient and effective audit process.

[11] Special consideration should be given to specific confidentiality agreements for joint state/FCC staff audits. No new provisions are required to accomplish this.

require independent auditors to sign confidentiality and nondisclosure agreements. Finally, the Commission should establish, by rule, the penalties that will apply in the event of a violation of Section 220(c).

IV. FORMAL COMPLAINTS

In 1993, the Commission amended the formal complaint regulations to limit the duplication and dissemination of materials obtained through discovery and deemed proprietary by the submitter.[12] While the amendments have given some protection to confidential information, the competitive telecommunications market encourages carriers to use the formal complaint discovery process to obtain sensitive, and otherwise unavailable, data

Increasingly, the formal complaint process deteriorates into a maze of discovery disputes. The complainant requests hundreds--sometimes even thousands--of documents, many of which have little or no relevance to the claim at issue, but all of which contain important and confidential business information. The defendant objects to the discovery. Both parties file briefs. The Enforcement Division then rules, then more discovery requests are propounded, more objections are filed, and the process goes on and on.

The NPRM acknowledges the current problems with the formal complaint procedure:

> We welcome suggestions as to how we can preserve the broad utility of the formal complaint process to elucidate the Commission's judgements regarding carrier conduct without either compromising

[12] 47 C.F.R. §1.731; see Amendment of Rules Governing Procedures to Be Followed When Formal Complaints Are Filed Against Common Carriers, 8 FCC Rcd 2614, 2621-22 (1993).

sensitive business data or miring complaint proceedings in protracted peripheral disputes involving confidentiality [13]

Unfortunately, no tinkering with the current rules will alleviate the delay and frustration caused by discovery abuses. Therefore, the Commission should *eliminate discovery entirely from the formal complaint procedure*.

While this approach may seem radical, it would not deny any party the right to full and complete adjudication of a controversy. Any aggrieved party always has the option of filing a lawsuit in either state or federal court. Such judicial proceedings would still afford all litigants the opportunity for full and complete discovery.

Eliminating discovery would, in effect, transform formal complaint proceedings into summary dispositions. If, in addition, the Commission were to set stringent deadlines upon the filing of answers and briefs, then it would be possible to comply with those provisions of the 1996 Act that require formal complaints to be fully decided within five months.[14]

Eliminating discovery would also obviate the need for elaborate rules protecting confidential information. The process would be streamlined enormously, and those parties desiring to delay a proceeding or to harass an opponent through abuse of the discovery process would be prevented from doing so at the Commission and could only attempt to do so at the courthouse.[15]

---

[13] NPRM at ¶50.

[14] 47 U.S.C. §208(b)(1).

[15] If discovery is eliminated, however, Commission Rules should be amended to allow the defendant in a formal complaint to remove the matter to state or federal court. Otherwise, the complainant could shield itself from discovery--in those few cases in which discovery by the defense is necessary--simply by filing a formal complaint.

V. CONCLUSION

As competition increases, all business data becomes increasingly sensitive, and the need for confidential treatment expands exponentially. If the Commission is to ensure that competition is reasonable and equitable, then parties must be given the opportunity to protect their proprietary data.

In tariff matters, the ILECs should no longer be required to support tariff filings with cost data. If the Commission does not revise its Rules to eliminate the submission of cost support, then the Commission should establish, by specific rule. that cost data is presumed confidential and will remain confidential. Parties requesting public dissemination of cost information should be required to state compelling arguments for release of the information. Even upon such a showing, the Commission should take great care that the requested information is protected from dissemination outside the specific tariff proceeding.

The Commission's draft protective order, attached as an Exhibit to the NPRM, is wholly insufficient to protect confidential information, primarily because it does not recognize different levels of confidentiality. The draft protective order is much less restrictive than similar orders employed in state jurisdictions. If the Commission's protective order is less restrictive, it will encourage parties to game the regulatory process and seek on the federal level what they have been denied on the state level.

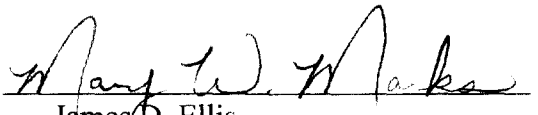
The Commission should not require LECs to submit formal requests for confidential treatment of information produced during audits. Such a requirement would make the audit process unworkable. The only time an audited carrier should be required to submit a request for confidentiality is after the Commission has received a request for inspection from a third party.

Discovery should be eliminated entirely from formal complaints, thereby streamlining the process and eliminating the need for any rules regarding the protection of confidential information. Parties wishing discovery could still avail themselves of judicial remedies.

The adoption of these proposals would provide adequate protection for confidential information and would encourage the market to function effectively and efficiently, as was the intent of the Telecommunications Act of 1996.

Respectfully Submitted,

SBC COMMUNICATIONS INC.

By 

James D. Ellis
Robert M. Lynch
David F. Brown
175 E. Houston, Room 1254
San Antonio, Texas 78205
(210) 351-3478

ATTORNEYS FOR SBC
COMMUNICATIONS INC.

Durward D. Dupre
Mary W. Marks
J. Paul Walters, Jr.
One Bell Center, Room 3520
St. Louis, Missouri 63101
(314) 235-2507

ATTORNEYS FOR SOUTHWESTERN BELL
TELEPHONE COMPANY

June 14, 1996

Exhibit A

DOCKET NOS. 12475 & 12481

APPLICATION OF SOUTHWESTERN BELL TELEPHONE COMPANY AND GTE SOUTHWEST, INC. FOR APPROVAL OF LRIC WORKPLAN PURSUANT TO SUBST. R. §23.91	§ § § § §	PUBLIC UTILITY COMMISSION OF TEXAS

PROTECTIVE ORDER

WHEREAS, Southwestern Bell Telephone Company ("Southwestern Bell") and GTE Southwest, Inc. ("GTE") have filed applications for approval of workplans pursuant to Substantive Rule §23.91 to be followed by performance of cost studies, and discovery may be requested seeking information and documents that Southwestern Bell and GTE consider to be subject to varying degrees of confidentiality, and as a condition to the production of said information and documents, Southwestern Bell and GTE have requested the Public Utility Commission of Texas ("Commission") to enter a Protective Order recognizing the confidentiality of the information and documents. This Protective Order shall apply to said workplans and subsequent cost studies that are prepared pursuant to the workplans.

Accordingly, this Protective Order is hereby approved and shall control the production of information and documents until such time as this Protective Order is modified by subsequent order.

Definitions

1. The term "party" as used in this Protective Order means any party to the Public Utility Commission of Texas Docket Nos. 12475 and 12481 and, for purposes of this Order during the pendency of this docket at the Commission, the Commission's General Counsel and Staff.

2. The term "Confidential Information" refers to all documents, data, information, studies and other materials furnished pursuant to requests for information or other modes of discovery, including, but not limited to, depositions and cost study information that are claimed to be trade secrets, confidential business information or information subject to an evidentiary privilege. "Confidential Information" shall include the term "Highly Sensitive Confidential Information" as defined herein. "Confidential Information" shall not include information contained in the public files of any federal or state agency that is subject to disclosure under the Texas Open Records Act (Tex. Government Code Chapter 552) or a similar statute. Nor shall it include information that, at the time it is provided through discovery in these proceedings or prior thereto, is or was public knowledge, or which becomes public knowledge other than through disclosure in violation of this Order. Nor shall it include information found by the Administrative Law judge, the Commission or a court of competent jurisdiction not to merit the protection afforded Confidential Information under the terms of this Order.

3. The term "Highly Sensitive Confidential Information" is a subset of "Confidential Information" and refers to information that a responding party claims is of such a highly sensitive nature that the making of copies of such information by a propounding party having access to such information as contemplated in Paragraph 9 of this Protective Order would expose the responding party to an unreasonable risk of harm. "Highly Sensitive Confidential Information" shall not include information found by the Administrative Law Judge, the Commission or a court of competent jurisdiction not to merit the protections afforded Highly Sensitive Confidential Information under the terms of this Protective Order. The term "Highly

Sensitive Confidential Information--Restricted" is a subset of the category of "Highly Sensitive Confidential Information" that involves information that is so confidential that its disclosure is limited to General Counsel and to Office of Public Utility Counsel ("OPUC").

Procedure - Generally

4. In the discovery or other proceedings or filings to be conducted or made in this docket, any party hereto may designate certain documents and information produced by such party as "Confidential." All such documents and information shall be clearly labeled to show that the documents are considered "Confidential." All Confidential Information shall be furnished pursuant to the terms of this Protective Order and shall neither be used nor disclosed except for the purpose of this proceeding or resulting proceedings before any judicial tribunal.

5. All Confidential Information produced pursuant to this Protective Order shall be made available solely to counsel for the parties, including in-house counsel, and witnesses or other persons working under the supervision of counsel. Parties to this proceeding who are not signatories hereto shall not be entitled to receipt of any Confidential Information.

6. Prior to giving access to Confidential Information as contemplated in Paragraph 5 above, to any person authorized to be given access pursuant to this Order, including attendance of depositions, counsel for the party seeking review of the Confidential Information shall deliver a copy of this Protective Order to such persons, and prior to disclosure, such person shall agree in writing to comply with and be bound by this Protective Order in the form of Exhibit A, attached hereto. Said counsel shall, at the time of the review of such Confidential Information, or as soon thereafter as practical, deliver to counsel for the party that produced the

Confidential Information a copy of Exhibit A as executed, which shall show each signatory's full name, permanent address and employer, and the party with whom the signatory is associated.

7. Each party producing Confidential Information and having an office or attorney's office in Austin shall designate an Austin location where all parties shall be permitted access to and review of such Confidential Information. Any such access and review shall be limited to regular business hours after reasonable notice by the requesting party. Each party producing Confidential Information and not having an office or attorney's office in Austin, Texas, shall produce such information for inspection by all parties at the Commission offices by prearranged appointment from 8 a.m. to 5 p.m. on Commission work days or at such other times as the Administrative Law Judge may designate.

With the exception of OPUC and General Counsel, each party shall maintain custody of its Confidential Information at a location other than the offices of the Commission, except as otherwise provided by this Protective Order. However, nothing in this Protective Order shall prohibit any party from maintaining, in the same office buildings where the Commission is located, an office in which to keep information claimed to be either Confidential Information or Highly Sensitive Confidential Information.

Procedure - Confidential Information

8. The procedures set forth in this paragraph apply with respect to production and review of information claimed to be Confidential Information, unless (1) the producing and reviewing parties agree otherwise or (2) as otherwise required by the provisions of this Protective Order, including but without limitation, Paragraph 10 relating to review by the General Counsel and OPUC.

On or before the date the response is due, two copies of information designated by the responding party as Confidential Information will be delivered to the party that requested the information, unless that information is voluminous. Unless otherwise ordered, voluminous information shall mean information which contains 200 pages or more. The two copies of the Confidential Information shall be provided to the requesting party's counsel of record or a consultant (or if no consultant, regulatory employees acting at direction of counsel) who has agreed in writing to be bound by this Protective Order. On or before delivery of the responses, the responding party shall file with the Commission and deliver to the requesting party a written statement which may be in the form of an objection indicating: (1) the reasons supporting the responding party's claim that the responsive information is subject to treatment as Confidential Information, and (2) that counsel for the responding party has reviewed the information sufficiently to state in good faith that the information merits the Confidential designation.

The information produced shall be organized in a manner that clearly identifies each document or portion thereof that is claimed to be Confidential. The producing party shall be responsible for producing the Confidential Information in a sealed envelope that is clearly marked on the outside as containing Confidential Information and that clearly specifies the numbers of pages contained therein.

The copies are to be made by or under the supervision of the personnel of the party who produced such document, who will affix a stamp to each item to be copied denoting the Confidential designation of the item. The stamp shall be affixed in such a manner so that the text of the Confidential Information is not obscured on either the original or any copies thereof.

Counsel of record for the person authorized hereunder who requested the copies shall sign a statement in the form of Exhibit B attached hereto verifying that the sealed envelope clearly marked as containing Confidential Information has been received and designating the name and address of the individual into whose custody the copies shall be delivered. The designated representative of the producing party shall also sign Exhibit B and verify to whom the sealed envelope was delivered. Access to said copies shall be limited to those persons defined in Paragraph 5 of this Order. No additional copies shall be made, unless the parties agree otherwise, or upon a showing of a good cause the Administrative Law Judge directs otherwise.

Persons who have agreed in writing to be bound by this Protective Order and are therefore permitted access to Confidential Information by this Order may take notes regarding such information as may be necessary in connection with this proceeding. Such notes shall be treated in the same manner as the Confidential Information from which the notes were taken.

Voluminous information designated as Confidential Information may be reviewed at the responding party's Austin location, as described in Paragraph 7 of this Protective Order.

Procedure - Highly Sensitive Confidential Information

9. The following procedures apply with respect to production and review of information claimed to be Highly Sensitive Confidential Information, unless (1) the producing and reviewing parties agree otherwise, or (2) as otherwise required by the provisions of this Protective Order, including but without limitation, Paragraph 10 relating to review by the General Counsel and OPUC.

On or before the date the response is due, the party producing information claimed to be Highly Sensitive Confidential Information shall file with the Commission and deliver to the party that requested the information, a written statement which may be in the form of an objection that includes the following information: (1) the identity of the party requesting the Highly Sensitive Confidential Information; (2) a verbatim recitation of those Requests for Information for which responsive information, in whole or in part, is deemed to be Highly Sensitive Confidential Information; (3) a description of the document or portion thereof that is allegedly too highly sensitive to disclose pursuant to the provisions of this Protective Order; (4) a written statement that explains why the information is Highly Sensitive Confidential Information; and 5) that counsel for the responding party has reviewed the information sufficiently to state in good faith that the information merits the Highly Sensitive Confidential Information designation.

Subject to the exceptions set forth in Paragraph 10, information claimed to be Highly Sensitive Confidential Information must be made available at the responding party's Austin, Texas, location on or before the date the response is due. The responding party to whom the request is made shall make that information available as specified in Paragraph 7. Persons permitted access to Highly Sensitive Confidential Information by this Order who have agreed in writing to be bound by the Protective Order may take limited notes regarding such Highly Sensitive Confidential Information as may be necessary in connection with this proceeding when required solely for the use and purpose of this Protective Order. Such notes shall be treated in the same manner as the Highly Sensitive Confidential Information from which the notes were taken.